IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FIRST CHOICE FEDERAL CREDIT UNION, on Behalf of Itself and All Others Similarly Situated, Plaintiff, vs. ARBY'S RESTAURANT GROUP, INC., Defendant.	Civil Action No.

CLASS ACTION COMPLAINT

Plaintiff First Choice Federal Credit Union ("Plaintiff" or "First Choice") by its undersigned counsel, individually and on behalf of a class of all similarly situated financial institutions, upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters, brings this action against Defendant Arby's Restaurant Group, Inc. ("Arby's" or "Defendant"), and states:

NATURE OF THE CASE

1. This is a class action arising out of a data breach involving Arby's. In or around October 2016, computer hackers began using malicious software known

as malware to access point-of-sale ("POS") systems at Arby's locations throughout the United States.

2. According to KrebsonSecurity, "Arby's said the breach involved malware placed on payment systems inside Arby's corporate stores, and that Arby's franchised restaurant locations were not impacted."[1]

3. In this data breach, the computer hackers stole data consisting of customers' debit and credit card information, including card numbers. This information was compromised because of Arby's acts and omissions and its overall failure to properly protect the payment card data of its customers.

4. In addition to Arby's failure to prevent the data breach, Arby's also failed to detect the breach for a period of nearly three months, and only learned of it after certain financial institutions reached out to KrebsonSecurity, which in turn informed Arby's.

5. Although Arby's has declined to disclose how long the malware was on its systems, a notice from PSCU, a Credit Union Service Organization, stated that the breach is estimated to have occurred between October 25, 2016, and January 19, 2017 (the "Arby's Data Breach"). *Id.*

[1] KrebsonSecurity, *Fast Food Chain Arby's Acknowledges Breach* (Feb. 9, 2017) https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/ (last visited Feb. 22, 2017).

6. A spokesperson for Arby's acknowledged that the Company was first notified by industry partners in mid-January about a breach at some stores. *Id.*

7. In a statement just issued by Arby's on February 16, 2017, the Company acknowledged that the breach had occurred:

> Arby's Restaurant Group, Inc. (ARG) was recently provided with information that prompted it to launch an investigation of its payment card systems. ARG immediately notified law enforcement and enlisted the expertise of leading security experts, including Mandiant. While the investigation is ongoing, ARG quickly took measures to contain this incident and eradicate the malware from systems at restaurants that were impacted.[2]

8. Had Arby's implemented reasonable processes and procedures to safeguard customer data, it is more likely than not that the breach would have been prevented.

9. The Arby's Data Breach forced Plaintiff and other financial institutions to: (a) cancel or reissue credit and debit cards affected by the Arby's Data Breach; (b) close or reopen customer accounts that were compromised; (c) stop payment or block transactions involving compromised accounts; (d) reimburse customers for the costs of unauthorized and fraudulent transactions involving compromised payment cards; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts.

---

[2] Arby's, *Statement Regarding Data Security Incident*, http://arbys.com/security/ (last visited Feb. 22, 2017).

10. In addition, the Arby's Data Breach caused Plaintiff and the members of the Class to lose revenue as a result of a decrease in card usage after the breach was disclosed to the public.

11. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including credit and debit card data and personal identifying information. Arby's failed to take steps to employ adequate security measures despite recent, well-publicized data breaches at large national retail and restaurant chains, including Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Wendy's, Dairy Queen, Noodles & Company, and Kmart.

12. The Arby's Data Breach was the inevitable result of Arby's inadequate data security measures. Despite the well-publicized and ever-growing threat of cyber breaches involving payment card networks and systems, Arby's failed to ensure that it maintained adequate data security measures that likely would have prevented the data breach and led to its earlier discovery.

13. Defendant exacerbated the situation, and the resulting injury to financial institutions, by failing to notify customers and the public in a timely manner after learning of the breach. Had Arby's promptly notified the public of

the data breach, less data would have been stolen and financial institutions would have been able to take earlier action to mitigate their damages.

14. This class action is brought on behalf of financial institutions throughout the country to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Arby's Data Breach and to obtain equitable relief. Plaintiff asserts claims for negligence, negligence per se, and declaratory and injunctive relief.

JURISDICTION AND VENUE

15. This Court has original jurisdiction of this action pursuant to the Class Action Fairness Act, 28 U.S.C §1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship from Arby's. There are more than 100 putative class members.

16. This Court has personal jurisdiction over Arby's because Defendant maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Arby's intentionally availed itself of this jurisdiction by accepting and processing payments for its foods and other services within Georgia.

17. Venue is proper under 28 U.S.C. §1391(a), because Arby's principal place of business is in this District and a substantial part of the events, acts, and

omissions giving rise to Plaintiff's claims occurred in this District. Venue is also proper in the Atlanta division.

PARTIES

18. Plaintiff First Choice Federal Credit Union is a federally chartered credit union with its principal place of business located in New Castle, Pennsylvania. First Choice issued Visa payment cards that were compromised by the Arby's Data Breach and as a result has suffered, and continues to suffer, injury, including, inter alia, incurring costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage. First Choice received a CAMS alert from Visa on or about February 7, 2017, informing it of the Arby's Data Breach, listing an "Exposure Window" of October 25, 2016 through January 19, 2017.

19. Defendant Arby's Restaurant Group, Inc. is a Delaware corporation with its principal place of business located at 1155 Perimeter Center, Suite 1200, Atlanta, Georgia 30338. According to its public statements, Arby's operates more than 3,300 company-owned and franchisee locations across the U.S. and worldwide.[3] Roughly one-third of those are corporate-owned stores.

[3] *See generally* http://arbys.com/press-center (last visited Feb. 22, 2017).

20. Arby's is a restaurant business that accepts payment for its goods and services through a point-of-sale network. Consumers swipe payment cards, which are issued by Plaintiff and the Class, at POS terminals to pay Arby's for its goods and services.

STATEMENT OF FACTS

21. A large portion of sales at Arby's locations are made to customers using credit or debit cards. A basic description of the various steps necessary to execute a credit/debit card transaction is as follows: (1) after the credit/debit card is swiped, the merchant (*e.g.*, Arby's) uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request for authorization to the institution that issued the payment card (*e.g.*, Plaintiff); (2) the issuing institution authorizes the payment and the merchant electronically forwards a receipt of the transaction to another financial institution, known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions on the merchant's behalf; (3) the acquiring bank forwards the funds to the merchant to satisfy the transaction and is then reimbursed by the issuing financial institution (*e.g.*, Plaintiff); and (4) finally, the issuing institution posts the debit or credit transaction to its customer's account.

22. Arby's is, and at all relevant times has been, aware that the payment card data it maintains is highly sensitive and could be used for nefarious purposes

by third parties, such as perpetrating identity theft and making fraudulent purchases.

23. Arby's is, and at all relevant times has been, aware of the importance of safeguarding its customers' payment card data and of the foreseeable consequences that would occur if its data security systems were breached, specifically, including the significant costs that would be imposed on issuers, such as Plaintiff, members of the Class, and others.

24. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected.

25. Recently, financial institutions have experienced an unprecedented number of Compromised Account Management System ("CAMS") alerts on their members' accounts from Visa and Account Data Compromise Alerts ("ADC alerts") on their members' accounts from MasterCard. CAMS and ADC alerts typically are issued by Visa and MasterCard when there is some event that jeopardizes the security of a financial institution's customers' accounts.

26. Numerous financial institutions have traced the large number of alerts issued for their customers' accounts and discovered a common thread: Arby's.

27. The number of CAMS and ADC alerts received by many financial institutions have been among the largest (meaning most cards compromised) CAMS or ADC alerts they have ever received for a single event.

28. An alert Plaintiff received estimates that the "exposure window" for the breach of Defendant's computer systems runs from October 25, 2016 to January 19, 2017, meaning Arby's failed to prevent or stop hackers from accessing its system and stealing cardholder data for almost three months.

29. The alert further indicates that both Track 1 and Track 2 data may have been compromised in the data breach. Track 1 and Track 2 data normally includes credit and debit card information such as cardholder name, primary account number, expiration date, and, in certain instances, PIN number.

30. Arby's has only made an official public announcement regarding the breach of its data processing systems. The announcement was made approximately four months after the breach began and one month after it ended. Arby's has not yet provided any specific information regarding the ultimate scope of the breach.

31. The Arby's Data Breach only become public when, on February 9, 2017, Brian Krebs, of KrebsonSecurity, a leading information security investigator, announced that he had reached out to Arby's after hearing from several financial institutions about a suspected breach at Arby's. In response to Mr. Krebs'

communication, Arby's informed Krebs that it recently remediated a breach involving malicious software installed on payment card systems at hundreds of its restaurant locations nationwide. Indeed, initial reports of the attack appear to have come from PSCU.[4]

32. According to Krebs, a spokesperson for Arby's said that Defendant was first notified by industry partners in mid-January about a breach at some of its locations. In a written statement to Krebs, Arby's said that the breach involved malware placed on payment systems inside Arby's corporate stores. There are over 1,000 corporate Arby's restaurants, although Arby's claims that not all of these restaurants were impacted by the Arby's Data Breach.[5]

33. Arby's still has yet to confirm how long the malware was on its data systems and how long hackers were able to steal Arby's customers' payment card information.

34. Arby's confirmed that the breach involved malware placed on payment systems inside Arby's corporate stores, but further stated that Arby's franchised restaurant locations were not impacted.

---

[4] https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/.

[5] *Id.*

35. The breach of Arby's data systems occurred through Defendant's POS network, where hackers installed malware that allowed them to steal payment card data from remote locations as a card was swiped for payment.

36. The Arby's Data Breach was made possible because Arby's failed to implement adequate data security measures to protect its POS network from the potential danger of a data breach, and failed to put in place reasonable systems to detect and prevent the breach and resulting harm that it has caused.

37. Defendant knew and understood the serious and real dangers associated with failing to implement adequate data security protection measures given the various high-profile data breaches that have occurred in the same way over the past few years, including data breaches of Target, Home Depot, and, most recently, Wendy's. Despite this knowledge, Defendant acted unreasonably and failed to adequately and reasonably protect the data of its customers.

38. In addition, the requirements of common law, industry standards, the FTC Act, and other authorities imposed a duty on Arby's to use reasonable care to protect its customers' sensitive financial data.

39. *Industry Standards.* The payment card industry (MasterCard, Visa, Discover Financial Services, and American Express), long before the Arby's Data Breach, issued Card Operating Regulations that: (1) are binding on Arby's; (2) required Arby's to protect cardholder data and prevent its unauthorized disclosure;

(3) prohibited Arby's from storing such data, even in encrypted form, longer than necessary to process the transaction; and (4) mandated that Arby's comply with industry standards.

40. The payment card industry has also set rules requiring all businesses, including Arby's, to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the hackers making it much more difficult for criminals to profit from what is stolen.

41. The set deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015, a deadline Defendant, on information and belief, did not meet.

42. Under the Card Operating Regulations that are binding on Defendant, businesses accepting payment cards but not meeting the October 1, 2015 deadline agree to be liable for damages resulting from any data breaches.

43. Further, the Payment Card Industry Security Standards Council promulgates minimum standards which apply to all organizations that store,

process, or transmit payment card data. These standards are known as the Payment Card Data Security Standards ("PCI DSS"). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

44. PCI DSS 3.1, the version of the standards in effect at the time of the Arby's Data Breach, sets detailed and comprehensive requirements for satisfying each of the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

45. Among other things, PCI DSS required Arby's to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix security vulnerabilities; assign unique

identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

46. Arby's was at all times fully aware of its obligations to protect customer data in light of its participation in the payment card processing networks and its daily collection and transmission of tens of thousands of sets of payment card data. Arby's was also fully aware that customers and financial institutions such as Plaintiff were entitled to, and did, rely on Arby's to use reasonable care and follow PCI DSS requirements in protecting its customers' sensitive financial information from data thieves.

47. While compliance with the PCI DSS is required as a minimum guarantee of protection, PCI DSS compliance in and of itself is insufficient. For example, Georgia Weidman, CTO and founder of Shevirah (a company that tests data security for retailers and other merchants), has stated that "[e]very company that has been spectacularly hacked in the last three years has been PCI complaint . . . . Obviously, based on that evidence, while a good step in the right direction, PCI is not sufficient to protect against breaches."[6]

48. *Section 5 of the FTC Act.* According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures

[6] Sean Michael Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, EWEEK (Aug. 19, 2016), http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html (last visited Feb. 22, 2017).

to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45.

49. In 2007, the FTC published guidelines that establish reasonable data-security practices for businesses, noting businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[7]

[7] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last visited Feb. 22, 2017).

51. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

52. *State Statutes.* Several states have enacted data breach statutes that require merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code §1798.81.5(b) and Wash. Rev. Code §19.255, or that otherwise impose data security obligations on merchants, such as Minnesota's Plastic Card Security Act, Minn. Stat. §325E.64. States have also adopted unfair and deceptive trade practices acts which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

53. Arby's failure to reasonably protect financial institutions' cardholder data violated all of these statutory and industry-imposed obligations and caused substantial damage to Plaintiff and the Class.

54. Had Arby's remedied the deficiencies in its IT systems, it likely would have prevented the Arby's Data Breach because virtually all data breaches are preventable. In fact, the *Online Trust Alliance*, a non-profit organization whose

mission is to enhance online trust, user empowerment, and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013, and that 89% of data breaches occurring in that year were avoidable.

55. Indeed, the fact that the Arby's Data Breach was not discovered for approximately three months demonstrates Arby's lack of safeguards and appropriate data security measures.

56. Plaintiff and the Class were required to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and Class members are not. Financial institutions bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

57. As a result of the Arby's Data Breach, Plaintiff and Class members have been forced to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their members. They have also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Class members and Plaintiff – as well as the account numbers on the face of the cards – were devalued.

58. The financial damages suffered by Plaintiff and members of the Class are massive and continue to increase.

CLASS ALLEGATIONS

59. Plaintiff brings this action on behalf of itself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Arby's while malware was installed on its payment card systems.

60. Excluded from the Class are Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and his/her Court staff.

61. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination

methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

62. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. whether Arby's engaged in the misconduct alleged;

b. whether Arby's failed to implement adequate data security measures to detect and potentially prevent the breach;

c. whether Arby's owed a duty to Plaintiff and the Class members and whether Arby's violated that duty;

d. whether Plaintiff and the Class members were injured and suffered damages or other ascertainable loss as a result of Arby's conduct; and

e. whether Plaintiff and the Class members are entitled to relief and the measure of such relief.

63. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the Arby's Data Breach. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendant's conduct and Plaintiff and the Class are asserting claims based on the same legal theories.

64. **Adequacy**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

65. **Superiority**: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Arby's, so it would be impracticable for members of the Class to individually seek redress for Arby's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

66. **Injunctive and Declaratory Relief**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

COUNT I
Negligence

67. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

68. Arby's owed an independent duty to Plaintiff and the members of the Class to take reasonable care in cardholder data, and to timely notify Plaintiff in the case of a data breach. This duty arises from multiple sources.

69. At common law, Arby's owed an independent duty to Plaintiff and the Class because it was foreseeable that Arby's data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from Arby's systems and misuse that information to the detriment of Plaintiff and the Class members, and that Plaintiff and the Class would be forced to mitigate such fraud by cancelling and reissuing payment cards and reimbursing their members for fraud losses.

70. Arby's common law duty also arises from the special relationship that existed between Arby's and the Class. Plaintiff and the Class entrusted Arby's with the cardholder data contained on the payment cards Plaintiff and the Class issued to their members. Arby's, as the holder and processor of that information, was the only party who realistically could ensure that its data systems were sufficient to protect the data it was entrusted to hold.

71. In addition to the common law, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45, further mandated Defendant to take reasonable measures to protect the cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates Arby's to take reasonable measures to protect any cardholder data Arby's may hold or process. The FTC publications and data security breach orders described above further form the basis of Arby's duty. In addition, individual states have enacted statutes based on the FTCA that also created a duty.

72. Arby's is also obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Arby's is bound. The industry standards create yet another source of obligations that mandate Arby's to exercise reasonable care with respect to Plaintiff and the Class.

73. Arby's, by its actions, has breached its duties to Plaintiff and the Class. Specifically, Arby's failed to act reasonably in protecting the cardholder

data of the members of Plaintiff and the Class members and did not have adequate systems, procedures, and personnel in place to reasonably prevent the disclosure and theft of its customer data.

74. As a direct and proximate result of Arby's conduct, Plaintiff and Class members have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They have also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

75. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence claim.

COUNT II
Negligence *Per Se*

76. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

77. Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants, and

other businesses such as Arby's of failing to use reasonable measures to protect cardholder data.

78. Arby's violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and not complying with applicable industry standards, including PCI DSS as described in detail, *supra*. Arby's conduct was particularly unreasonable given the nature and amount of cardholder data it obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions.

79. Arby's violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence *per se*.

80. Plaintiff and the Class members are within the class of persons that Section 5 of the FTCA (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. In addition, Plaintiff and many Class members are credit unions, which are organized as cooperatives whose members are consumers.

81. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their

failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class members.

82. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

83. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence *per se* claim.

COUNT III
Declaratory and Injunctive Relief

84. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

85. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad

authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

86. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the cardholder data of the members of Plaintiff and the Class. Plaintiff alleges Arby's actions (and inaction) in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff continues to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class members have issued.

87. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Arby's continues to owe a legal duty to secure its customers' personal and financial information – specifically, including information pertaining to credit and debit cards used by persons who made purchases at Arby's restaurants – and to notify financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Arby's continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Arby's ongoing breaches of its legal duty continue to cause Plaintiff harm.

88. The Court should also issue corresponding injunctive relief requiring Arby's to employ adequate security protocols consistent with industry standards to protect its customers' personal and financial information.

89. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Arby's data systems. The risk of another such breach is real, immediate, and substantial. If another breach of Arby's data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and it will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff as the result of a data breach, which include monetary damages that are not legally quantifiable or provable, and reputational damage.

90. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Arby's if an injunction is issued. Among other things, if

Arby's suffers another massive data breach, Plaintiff and the members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Arby's of complying with an injunction by employing reasonable data security measures is relatively minimal and Arby's has a pre-existing legal obligation to employ such measures.

91. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

92. Wherefore, Plaintiff, on behalf of itself and on behalf of the other members of the Class, requests that this Court award relief against Arby's as follows:

A. An order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

B. Awarding Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;

C. Enter a declaratory judgment in favor of Plaintiff and the Class as described above;

D. Grant Plaintiff and the Class the injunctive relief requested above;

E. Awarding attorneys' fees and costs; and

F. For such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

93. Plaintiff hereby demands a jury trial for all of the claims so triable.

DATED: February 24, 2017

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS
CANFIELD & KNOWLES, LLC
1355 Peachtree St., NE, Suite 1900
Atlanta, Georgia 30309-3238
Telephone: 404-881-8900
kcanfield@dsckd.com

JOSEPH P. GUGLIELMO
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
jguglielmo@scott-scott.com

ERIN G. COMITE
STEPHEN J. TETI
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
156 South Main St.
P.O. Box 192
Colchester, CT 06415
Telephone: 860-537-5537
ecomite@scott-scott.com
steti@scott-scott.com

Counsel for Plaintiff

CERTIFICATION

The undersigned hereby certifies, pursuant to Local Civil Rule 7.1D, that the foregoing document has been prepared with one of the font and point selections (Times New Roman, 14 point) approved by the Court in Local Civil Rule 5.1B.

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS
CANFIELD & KNOWLES, LLC
1355 Peachtree St., NE, Suite 1900
Atlanta, Georgia 30309-3238
Telephone: 404-881-8900
kcanfield@dsckd.com

Counsel for Plaintiff